

Fareit Malware Analysis using static and dynamic method

What is Fareit?

This form of malware was discovered in 2012, but has continued modifying throughout the years to bypass anti-virus protection. It is an information stealer that targets FTP credentials, email passwords and browser stored passwords. During dynamic analysis, it is observed all of the above being performed after the malware disabled local security tools.

How it is spreading to the crowd?

The most recent Fareit malware threat is being distributed via a phishing attack. A phishing attack is an email with a malicious link or attachment, designed to make you click on those links/attachments. This most recent phishing attack includes malicious executable disguised as a DOC, XLS, ISO, PPT file attachment, which includes the malware. Once the user downloads the Attachment, their computer becomes infected and the malware scans for any credentials that may be of value. This may range from banking information, various account login credentials, administrative credentials, etc.



Fareit Static Analysis:

SHA256: *ac0d0cf7eae9d4c3208a8d8ebf917a09c432fbc22daf7690698cd872966ee20e*

File General information:

File: ac0d0cf7eae9d4c3208a8d8ebf917a09c432fbc22daf769069cd872966ee20e

Property	Value
File Name	E:\...ac0d0cf7eae9d4c3208a8d8ebf917a09c432fbc22daf769069...
File Type	Portable Executable 32
File Info	No match found.
File Size	136.00 KB (139264 bytes)
PE Size	136.00 KB (139264 bytes)
Created	Saturday 01 September 2018, 09.19.11
Modified	Saturday 01 September 2018, 09.19.11
Accessed	Saturday 01 September 2018, 09.20.25
MD5	5B2FC87246470B71DD26CF65654CD5AB
SHA-1	51011887F6B9C7D9F7CA603801C895AA1FD65180

Property	Value
Empty	No additional info available

- No information related to Company Name, File Description, Legal Copyright, Product Version ext. (suspicious)

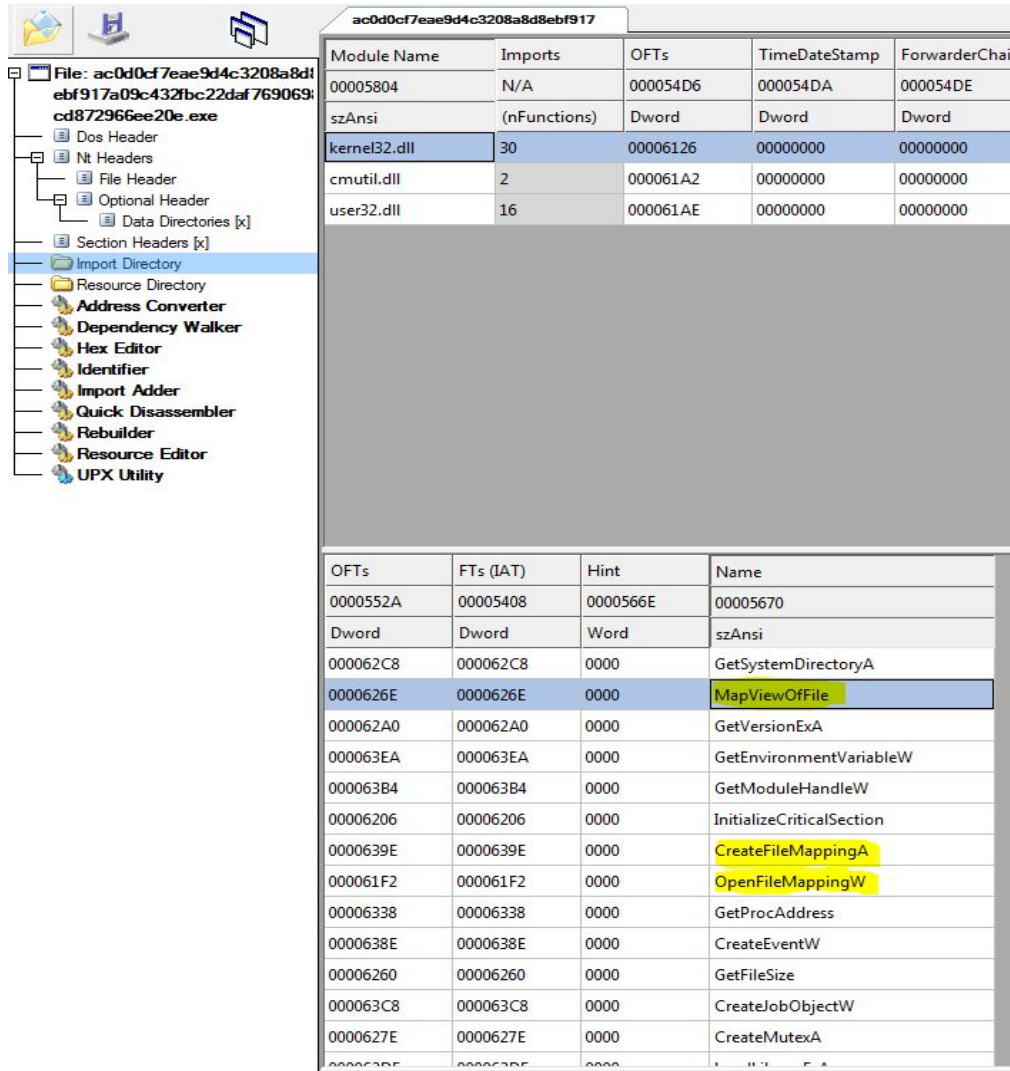
File Section headers:

File: ac0d0cf7eae9d4c3208a8d8ebf917a09c432fbc22daf769069cd872966ee20e

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
text1	00004FBF	00001000	00005000	00000400	00000000	00000000	0000	0000	60000020
.zdata	00000BBA	00006000	00000C00	00005400	00000000	00000000	0000	0000	C0000040
.zdata	000002BA	00007000	00000400	00006000	00000000	00000000	0000	0000	C0000040
.rsrc	0001BAF0	00008000	0001BC00	00006400	00000000	00000000	0000	0000	40000040

- Odd looking Non-Standard sections name: text1, odata, .wdata (suspicious)

File Import Directory:



File: ac0d0cf7eae9d4c3208a8d1ebf917a09c4321bc22daf769069cd872966ee20e.exe

Module Name	Imports	OFTs	TimeStamp	ForwarderChain
00005804	N/A	000054D6	000054DA	000054DE
szAnsi	(nFunctions)	Dword	Dword	Dword
kernel32.dll	30	00006126	00000000	00000000
cmutil.dll	2	000061A2	00000000	00000000
user32.dll	16	000061AE	00000000	00000000

OFTs	FTs (IAT)	Hint	Name
0000552A	00005408	0000566E	00005670
Dword	Dword	Word	szAnsi
000062C8	000062C8	0000	GetSystemDirectoryA
0000626E	0000626E	0000	MapViewOfFile
000062A0	000062A0	0000	GetVersionExA
000063EA	000063EA	0000	GetEnvironmentVariableW
000063B4	000063B4	0000	GetModuleHandleW
00006206	00006206	0000	InitializeCriticalSection
0000639E	0000639E	0000	CreateFileMappingA
000061F2	000061F2	0000	OpenFileMappingW
00006338	00006338	0000	GetProcAddress
0000638E	0000638E	0000	CreateEventW
00006260	00006260	0000	GetFileSize
000063C8	000063C8	0000	CreateJobObjectW
0000627E	0000627E	0000	CreateMutexA

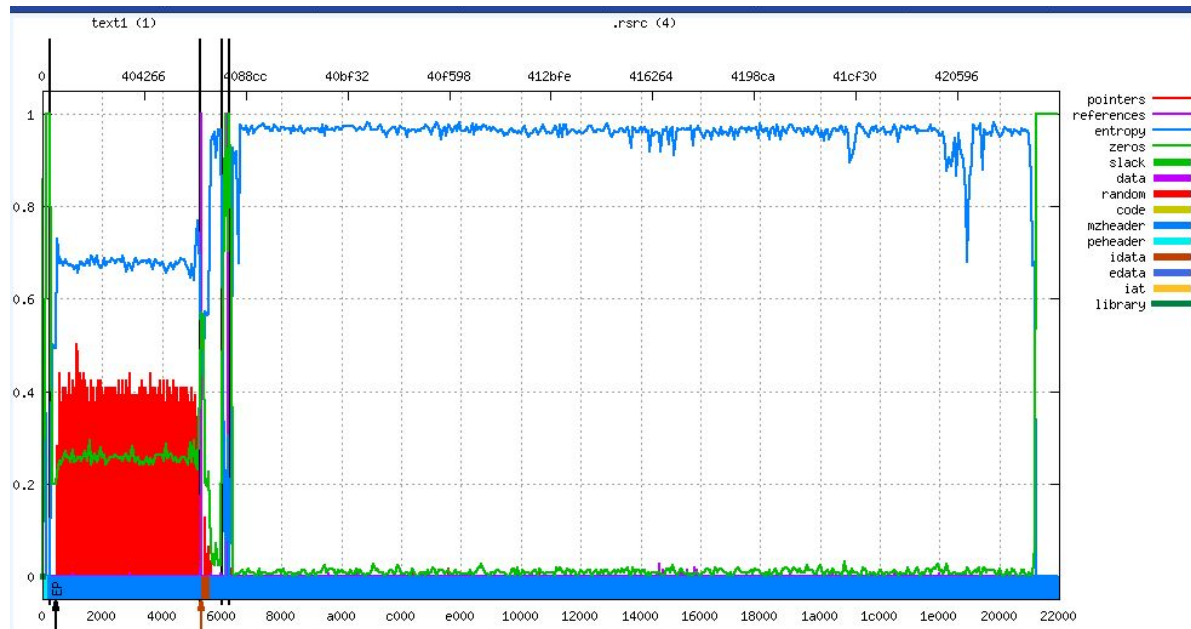
- It is importing some functions related to File mapping.

MapViewOfFile: Maps a view of a file mapping into the address space of the calling process.

CreateFileMappingA: Creates or opens a named or unnamed file mapping object for a specified file.

OpenFileMappingW: Opens a named file mapping object.

File Heu:



- File's Resource section is very large and dens, probably having encrypted data

Contact.verma7@Gmail.com

Address	Disassembly	Comment	Registers (32Neut)
00230562	00 PUSHD EAX		ERR 16408502
00230568	83EB 0A SUB EAX,0A		ECX 0001A500
0023056D	55 RCX24196 XOR EAX,RCX24196		EDX 77B72007
00230570	2BC2 SUB EAX,EDX		ERR 00400000
00230572	5A POP EDI		ESI 0010FF1C
00230575	AB STOS DWORD PTR ES:[EDI]		ERR 00400000
0023057A	83EB 03 XOR EAX,03		EDI 00230608
00230577	72 DB LOOPD SHORT 00230554		ESI 00240004
00230579	61 POPAD		EDI 00240000
00230570	C3 RETN		ERR 00230567
00230570	6633F6 XOR SI,SI		C 0 SS 002B 32bit 0(CFFFFFFF)
0023057E	66BA 4D5A MOV DX,5A4D		P 1 SS 002B 32bit 0(CFFFFFFF)
00230582	66D0 LODS WORD PTR DS:[ESI]		A 0 SS 002B 32bit 0(CFFFFFFF)
00230584	6633D0 XOR DX,AX		Z 0 DS 32bit 0(CFFFFFFF)
00230587	74 04 JC SHORT 00230592		S FS 002B 32bit 7(FED00000)
00230589	81EE 01100000 SUB ESI,10001		T 0 GS 002B 32bit 0(CFFFFFFF)
0023058B	4E DEC ESI		D 0
00230590	5A JMT SHORT 0023057E		0 0 LastErr ERROR_SUCCESS (00000000)
00230592	8D5E FE LEA EBX,DWORD PTR DS:[ESI-2]		EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
00230595	84FF TEST BH,BH		MM0 0.0 0.0
00230597	75 F0 JNZ SHORT 00230589		MM1 0.0 0.0
00230599	8976 30 MOV ESI,DWORD PTR DS:[ESI+30]		MM2 0.0 0.0
0023059C	66BA 5045 MOV DX,4550		MM3 0.0 0.0
002305A0	0D341E LEA ESI,DWORD PTR DS:[ESI+EBX]		MM4 0.0 0.0
002305A2	66D0 LODS WORD PTR DS:[ESI]		MM5 0.0 0.0
002305A5	6633D0 XOR DX,AX		MM6 0.0 0.0
002305A8	75 0F JNC SHORT 00230589		MM7 0.0 0.0
002305AB	C3 RETN		
002305AC	61 PUSH EAX		
002305AC	33C9 XOR ECX,ECX		
002305AE	41 INC ECX		
002305AF	2BC2 SUB EAX,EDX		
002305B1	70 04 JC SHORT 002305B7		
002305B3	74 02 JC SHORT 002305B7		
002305B5	EB F7 JMP SHORT 002305AE		
002305B7	330A XOR EAX,AX		
002305B9	8BC2 ADD EAX,EDX		
002305BB	E2 FC LOOPD SHORT 002305B9		
002305BD	59 POP ECX		
002305BE	C3 RETN		
002305BF	8B7D 74 MOV EDI,DWORD PTR SS:[EBP+74]		
002305C2	60 04 PUSH 000		
002305C4	60 00100000 PUSH 0000		
002305C9	77 PUSH EDI		
002305C8	60 00000000 PUSH 0		
002305D0	5A XOR SI,SI		

[illegible]

002B0554	3B75 64	CMP ESI,DWORD PTR SS:[EBP+64]
002B0557	75 0D	JNZ SHORT 002B0566
002B0559	0375 68	ADD ESI,DWORD PTR SS:[EBP+68]
002B055C	037D 68	ADD EDI,DWORD PTR SS:[EBP+68]
002B055F	2B4D 68	SUB ECX,DWORD PTR SS:[EBP+68]

```
002B0562 85C9      TEST ECX,ECX
002B0564 74 13      JE SHORT 002B0579
002B0566 AD        LODS DWORD PTR DS:[ESI]
002B0567 50        PUSH EAX
002B0568 83E8 0A    SUB EAX,0A
002B056B 35 AC324196 XOR EAX,964132AC
002B0570 2BC2      SUB EAX,EDX
002B0572 5A        POP EDX
002B0573 AB        STOS DWORD PTR ES:[EDI]
002B0574 83E9 03    SUB ECX,3
002B0577 ^E2 DB     LOOPD SHORT 002B0554
002B0579 61        POPAD
```

It decrypt's an executable file SHA 1: bb5d9b8aee93ef92cea52849b17f57bb4e3c0306

Behavior of the base file is suspicious itself, which is dropping another executable into the memory dump.

Farelt Dynamic analysis:

I have executed the file into safe environment and found some results:

After execution I have gathered data of file's Properties -> Strings -> strings and found some suspicious looking string form there:

- String Related to Passwords, Hostname

```
30  ]]]
31  HostName
32  PortNumber
33  UserName
34  Password
```

- Strings related to embedding a executable file in tempbuffer.dat


```

50  %APPDATA%\purple\accounts.xml
51  %TEMP%\tempbuffer.dat
52  MZP
53  This program must be run under Win32
54  CODE
55  `DATA
56  BSS
57  .idata
58  .reloc
59  P.rsrc
60  .idata
61  .reloc
62  P.rsrc
63  Char
64  Byte

```

- Found Functions related to Find first file, Excessive number of FindFirstFile calls (suspicious)

```

313 FindFirstFileW
314 FindNextFileW

```

- Found functions related to Hashing. (suspicious)

```

345 CryptAcquireContextA
346 CryptCreateHash
347 CryptHashData
348 CryptGetHashParam
349 CryptDestroyHash
350 CryptReleaseContext

```

The CryptCreateHash function initiates the hashing of a stream of data.

- Function to get keyboard layout.

```

354 GetKeyboardLayoutList

```

- Having Strings related to Browsers, email applications, Chat applications.

```

469 MozillaBased

```

```

521 InternetExplorer

```

```

534 Server
535 Outlook

```

```

652 Skype
653 Telegram
654 D877F783D5*,map*
655 %appdata%\Telegram Desktop\tdata\

```

- Having Strings Related to bit coin wallet related keywords.

```

620 %APPDATA%\
621 wallet.dat
622 \wallet.dat
623 electrum.dat
624 \electrum.dat
625 .wallet
626 \.wallet
627 %APPDATA%\MultiBitHD
628 mbhd.wallet.aes
629 \MultiBitHD\
630 \mbhd.wallet.aes
631 \mbhd.checkpoints
632 mbhd.checkpoints
633 \mbhd.spvchain
634 mbhd.spvchain
635 \mbhd.yaml
636 mbhd.yaml
637 wallet_path
638 Software\monero-project\monero-core
639 \Monero\
640 .address.txt
641 .keys
642 strDataDir
643 Software\Bitcoin\Bitcoin-Qt
644 \BitcoinBitcoinQT\wallet.dat
645 CPU Model:
646 jjjjjjjj
647 UTC+
648 Ajj
649 Coins
650 Coins\Electrum
651 %appdata%\Electrum\wallets\

```

- Having some base64 encoded strings:

Before decryption

```

809 U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWxs
810 RGlzcGxheU5hbWU=
811 U29mdHdhcmVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cVW5pbnN0YWxsXA==
812 RGlzcGxheVZlcnNpb24=

```

After decryption

```

809 Software\Microsoft\Windows\CurrentVersion\UninstallDisplayName
810 Software\Microsoft\Windows\CurrentVersion\Uninstall\

```

- Got a suspicious URI(which is malware repo categorized) (malicious connection)

```

916 system-check.xyz/index.php

```

- Probably saving all credentials to below file.


```
919 PasswordsList.txt
```

- Probably creating a JSON object to post data through the above URI

```
923 ip-api.com/json
924 "query": "
925 "countryCode": "
926 ip.txt
927 System.txt
928 reportdata=<info
929 </info
930 <pwds
```

From the above Strings, it does have a credential stealing + bitcoin related data stealing properties. Those are same as Fareit malware family.

Because of its anti-analysis feature I am not able to execute the malware to its full potential. But above analysis is enough to prove sample as a Fareit malware family.